Military CNO Training

January 2019

OnNet
#For advanced cyber methods

STATEMENT OF DOCUMENT CONFIDENTIALITY

The content of this report is **OPEN FOR PUBLIC**

Military CNO Training Course VERSION NO: 204 //PUBLIC

EXECUTIVE SUMMARY

Countries in Africa are rapidly approaching information age surge such that the military and intelligence services do require military modernization programs that fundamentally transform Law Enforcement Agencies (LEA) and Intelligence Communities (IC) capabilities to fight high tech wars with growth of its MMI. As the ratio number of deployed officers increases especially on networked forces, the capable of communication across service arms and intelligence, the effort to grow cyber domain capabilities further for a fully networked architecture capable of coordinating military operations on land, sea, air, space and cyber is advocated. Information dominance during war is a precursor for overall success in a conflict with the goal to establish control of an adversary's information flow and maintain the dominance attained in the battlefield. With the need of information collection against adversaries for support of military missions, the growing importance of comprehensive Computer Network Operations techniques is required for future support of strategic intelligence collection objectives to lay the foundation of potential future conflicts.

With this training outline, the military will equip and train it forces, on the use of variety of several information operations tools to support CNO operations during intelligence collection and dominance in cyber space.

Contents

PART A: Definitions

AD	Active Directory
AFT	Advanced Financial Threat
APT	Advanced Persistent Threat
ATRR	Advanced Tactical Rapid Response
C2	Command and Control.
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CNO	Computer Networks Operation (CNA, CNE, CND)
COMINT	Computer/Communication Intelligence
CTI	Cyber Threat Intelligence
DARE	Deep analysis and Reverse engineering
DITU	Data Interception Technology Unit
DC	Domain Controller
DFIR	Digital Forensics and Incidence Response
EDR	Endpoint Detection and Response
IMM	Imminent Methods
JOC	Joint Operations Centre
MMI	Major Military Innovation
OSINT	Open Source Intelligence
PE	Portable Executable
RAT	Remote Access Tool
RE	Reverse Engineering
ROE	Rules of Engagement
SIEM	Security, Information and Event Management
SIGINT	Signals Intelligence
Threat groups	East African Financial threat groups, Forkbombo, Corezeta with GrayWire and Silentcards
TTPs	Tactics, Techniques and Procedures
UnSub	Unknown Subject

0.0 OBJECTIVES

The CNO training has the following objectives:

a/ Understand all the five pillars of information operations, that is Computer Network Operations (CNO) aka Cyber, Electronic Warfare (EW), Military Deception (MILDEC), Operations Security (OPSEC), Psychological Warfare (PSYOP) aka MISO.

b/ Experiment the CNO Pillar for information operations by encompassing attack, defend and exploit.

c/ Collective establishment of Computer Network Exploitation (CNE), Computer Network Attack (CNA) and Computer Network Defense (CND).

d/ CNO Tooling especially for Command and Control.

1.0 TRAINING SCOPE

Being in the position to deliver actionable intelligence collected at Rest or even in Transit can be a natural transitional of foreign or local intelligence collection mission of SIGINT and COMINT.

CNE for the class will include and grouped into:

a) Collection Activities
b) Enabling Activities

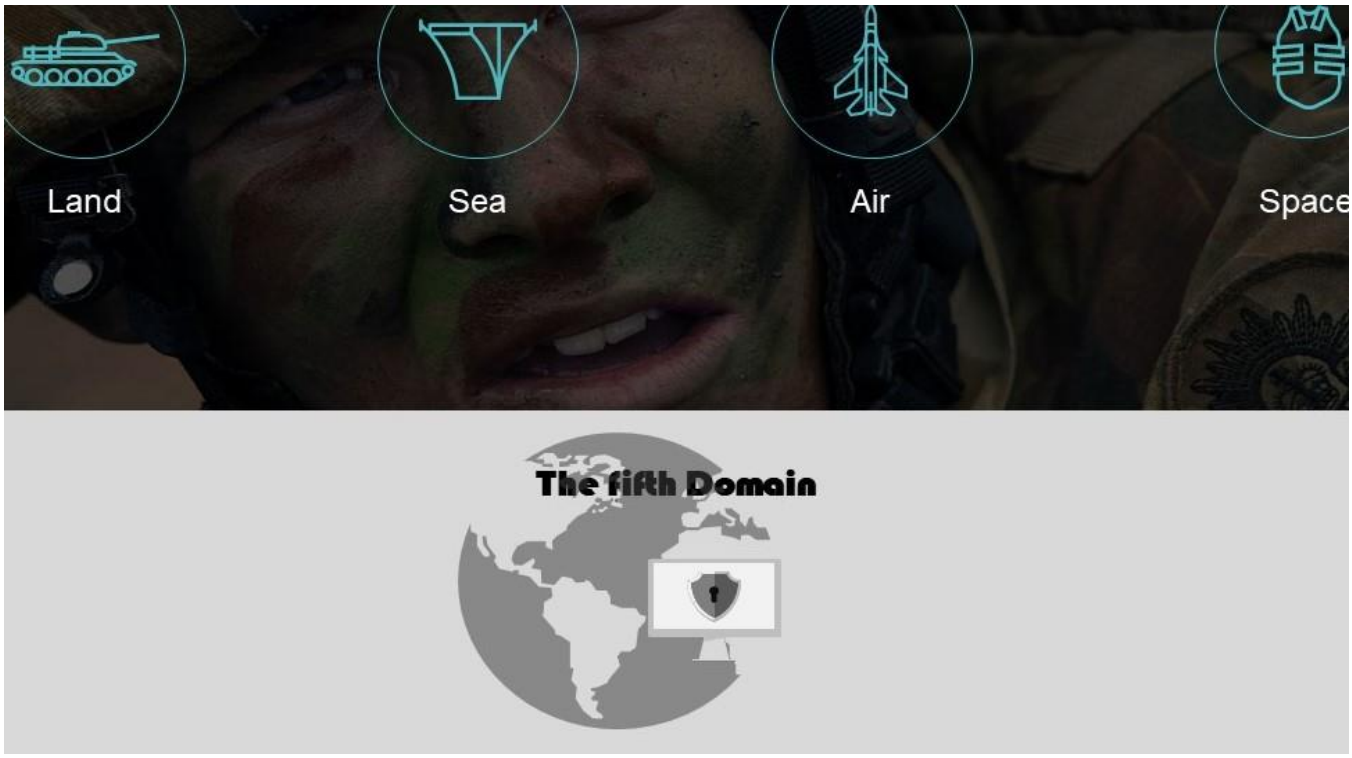
2.0 PREREQUISITES

All the students should have basic understanding of Windows and Linux Command line. With that, additional understanding of TCP/IP and some programming background is equally essential.

To get the most value out of this course, students are required to bring their own laptops to connect directly to the set-up lab at the barracks. Its students responsibly that the laptop is running Linux and is properly configured with all the drivers necessary to connect both Ethernet and Wireless environment at the Cyber Range.

3.0 COURSE SYLLABUS

The CNO training is extensively technical with a requirement of exposing the military officers in-charge of SIGINT to collect and facilitate active and actionable intelligence even before it leaves the devices used by the adversaries.

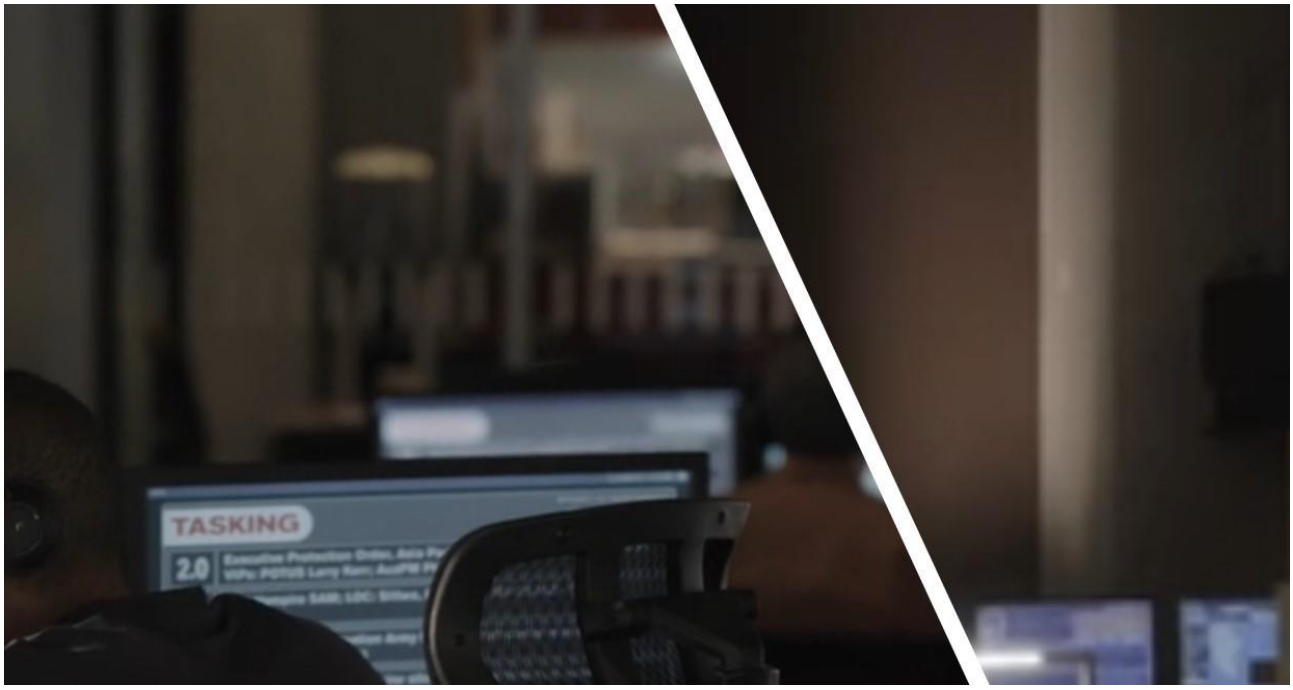


204.1 Network Security Essentials

The key to get into a computer is through a network, though sometimes sensitive services are usually disconnected from the internet. This class gives you hands on experience on basic operations to target and penetrate a network with basic Opensource tools. Most of the time opensource can easily be caught during missions and is undesirable for OPSEC but understanding how they are developed and deployed is an essential step in building CNO Units for combative and collection of data during peacetime and wartime.

204.2 Developing Cyber Espionage Tools and Extensive Cyber Weaponry

Underpinning CNE endpoints capabilities for our officers during CNO missions, this class will explore ways and means to plan, equip and conduct endpoint operations that actively compromised otherwise intractable targets and complement programs that passively eavesdrop on communication links.



The training on Endpoints CNE will include how to set up the Cyber range for practical operations during down range exercises. With range up, the activities shown in the class, will include surreptitious virtual or physical access to create and sustain a presence inside targeted systems or facilities. These systems will be targeted electronically thus collection of data covertly is deployed for mission requirements.
Student will learn how to cloak system logs during CNE and Housekeeping strategy for future access.

CNO Tool contrivance a special class, in CNO Tooling class is encouraged which includes full warfare package, either for loaders, loggers, injectors or fully packaged stage one or stage two implants when targeting an infrastructure. Sometimes during such operations, remote operations to target systems can be close to impossible and students are trained how to attain close-access operations with use of HUMINT toolset.

204.3 Researching & Re-Development of Cyber-Command's Kill Chain

This cybercom kill chain conceptual framework for warfare was developed by a team at ICT Authority (KE) for cyber operations against offenders who attacked and penetrated Government of Kenya infrastructure. This Kill chain was enacted and used during CNO Operations for attribution of actors and collection of intelligence on a targeted infrastructure for defend forward operations, to detect foreign government cyber operations and to support other technical services needed by other authorities.

This framework was maintained by a strong focus on R&D to counter cyber efforts and non-kinetic capabilities on mission to deny enemy access to information essential for continued combat operations and SIGINT/COMINT collection. The student will learn this framework and engage in combative readiness to operate in cyber space for mission integration capabilities, sustain covert domestic and foreign collection, defend against increasing cyber threats, and build a secure infrastructure capable of huge covert data exfiltration, command & control, and CNO operators capability of locating high priority targets that use evolving security when on cyber domain.

With diverse knowledge of CNO toolset contrivance during the latter classes, the students will operate in cyber space for prosecution of varied CNO missions with full understanding of OPSEC pillar, constituted in Information Operations.

4.0 AUTHOR STATEMENT

[redacted] Government of Kenya ICT infrastructure. The first incidence I responded to was [redacted] where they were exfiltrating documentations needed for their expansion in transport industry. During the later ensuing operations, cybercom had to create its own capability not only to counter cyber operations from nation states, but to combat domestic Advanced Financial Threats. During this duration cybercom kill chain was [redacted] Online Operations Action Team (OOAT) [redacted] On leaving Cyber Command I joined a Defense Intelligence Contracting Firm that runs CNO operations against Financial Threats in East Africa and support several Cyber Missions in Europe group office. As of now, the company capabilities have expanded to other countries across the world due our partnership with several stakeholders,

This document has been released to the Public since version 205 will be out as a class online under OnNet group and Cyber Ranges with much more current CNO Methodologies.